

平成 28 年度 秋期 情報セキュリティスペシャリスト試験 解答例

午後 I 試験

問 1

出題趣旨	
IoT (Internet of Things) への取組みが進み、モノとモノがつながることによるリスクの増大が予想されている。	
本問では、IoT へのセキュリティ対策を進める上で基本となる、組込み機器のセキュリティ対策に焦点を当て、組込み機器に発生しがちな情報セキュリティインシデントを踏まえ、インシデント対応やセキュリティ対策に必要なとなる知識、能力を問う。	

設問	解答例・解答の要点		備考
設問 1	a	エ	
	b	ア	
設問 2	(1)	c x1.x2.x3.x4 d y1.y2.y3.y4	
	(2)	パスワード認証を無効化し、公開鍵認証を使用する。	
設問 3	(1)	e 送信元 IP アドレスを監視端末の IP アドレスに限定	
	(2)	中間者攻撃による通信内容の盗聴	
	(3)	作成時 秘密鍵を使用してイメージファイルにデジタル署名を付与する。 更新時 公開鍵を使用してイメージファイルのデジタル署名を検証する。	
	(4)	LTE ルータにログインしてファイルシステムの中から見つける。	

問 2

出題趣旨	
依然として報告件数が減らないバッファオーバーフロー脆弱性 ^{ぜい} についての問題である。状況設定では開発ベンダとしているが、ソフトウェア開発業務に従事していなくても、今日の情報セキュリティスペシャリストならば、単なるキーワードの理解だけではなく、そのメカニズムと具体的対策も知っておくべきものである。	
本問では、それらを問う問題と共に、ソフトウェア開発における脆弱性対策全般についての取組みも問う。	

設問	解答例・解答の要点		備考
設問 1	a	ア	
	b	イ	
	c	ウ	
	d	エ	
設問 2	(1)	呼出し元関数への戻りアドレス	
	(2)	ア sample2	
設問 3	(1)	ウ	
	(2)	23	
	(3)	イ, オ	
設問 4	(1)	ヒープメモリの確保方法が、メモリ確保のライブラリによって違うから	
	(2)	ヒープ領域を書き換える行為を防止できないから	

問3

出題趣旨	
<p>昨今、特定企業を狙った標的型の電子メールを利用した攻撃の被害が多発しており、マルウェア対策の強化が求められている。</p> <p>本問では、PC におけるプログラムの起動禁止設定やプロキシサーバにおけるフィルタリング機能とプロキシ認証機能を用いて、マルウェアに対応する方法を考える能力を問う。</p>	

設問	解答例・解答の要点		備考
設問 1	a	エ	
設問 2	(1)	b	イ
		c	オ
	(2)	プログラムの内容を変え、かつ、プログラム名を変える場合	
設問 3	(1)	送信元 IP アドレスがプロキシ 1 の IP アドレスとなるので	
	(2)	d	オ
設問 4	(1)	Web ブラウザからプロキシサーバへの通信を盗聴して認証情報を取得し、プロキシサーバに送信する。	
	(2)	URL フィルタリング機能	ホワイトリストに業務に必要かつ安全であることを確認した URL を設定する。
		カテゴリ単位フィルタリング機能	業務に不要であるカテゴリを遮断する。